



MBSE Methodology for FM System Design

(Model Based System Engineering Methodology for Fault Management System Design)

Lui Wang, Michel Izygon*, Ph.D., Shira Okon*/ ER6
Spacecraft Software Engineering Branch, *Tietronix Software
JSC/NASA

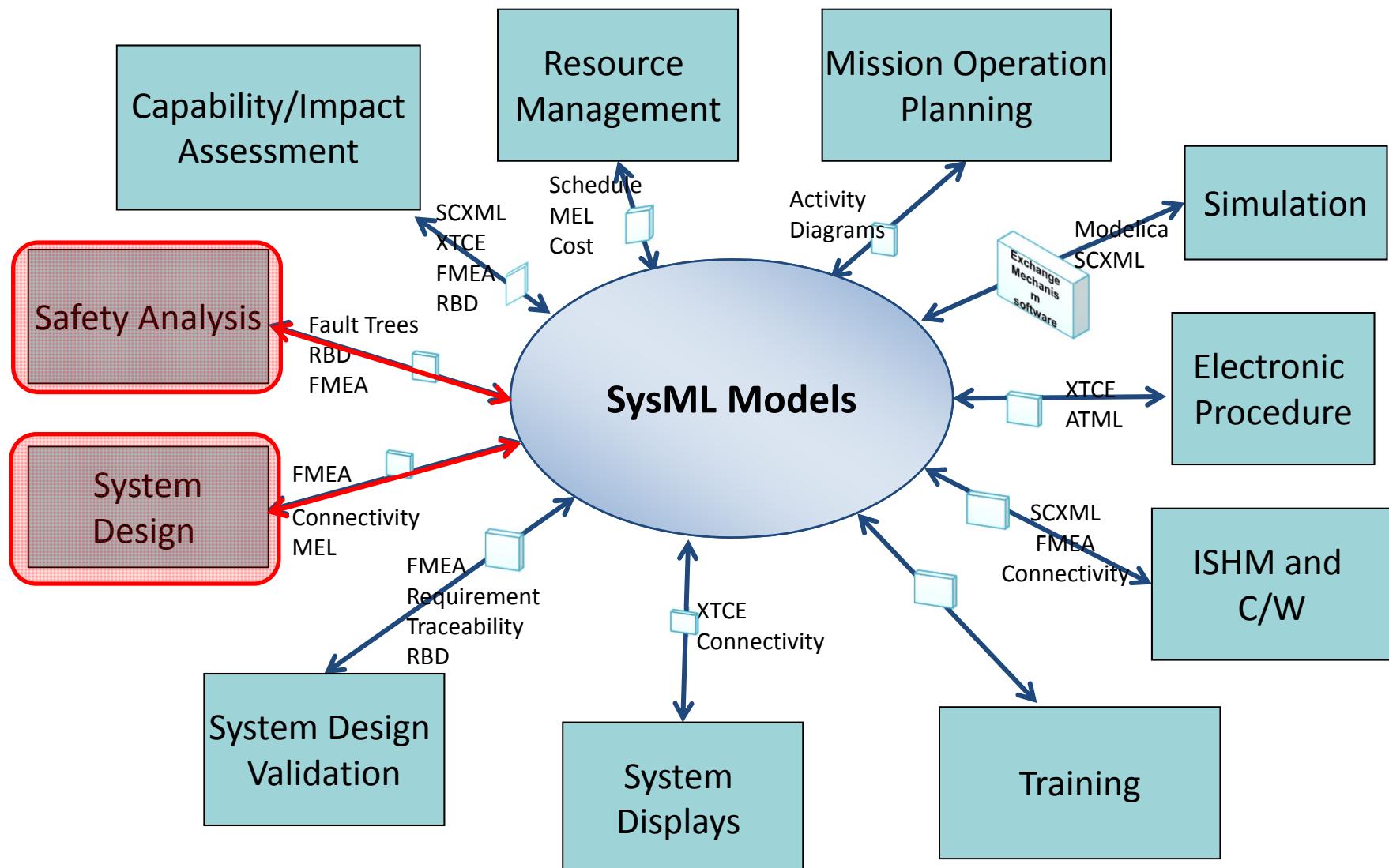
Magdy Bareh, Castet, Jean-Francois, Nunes, Jeffery, Lorraine Fesq
JPL/NASA

January 29, 2015



MBSE Context

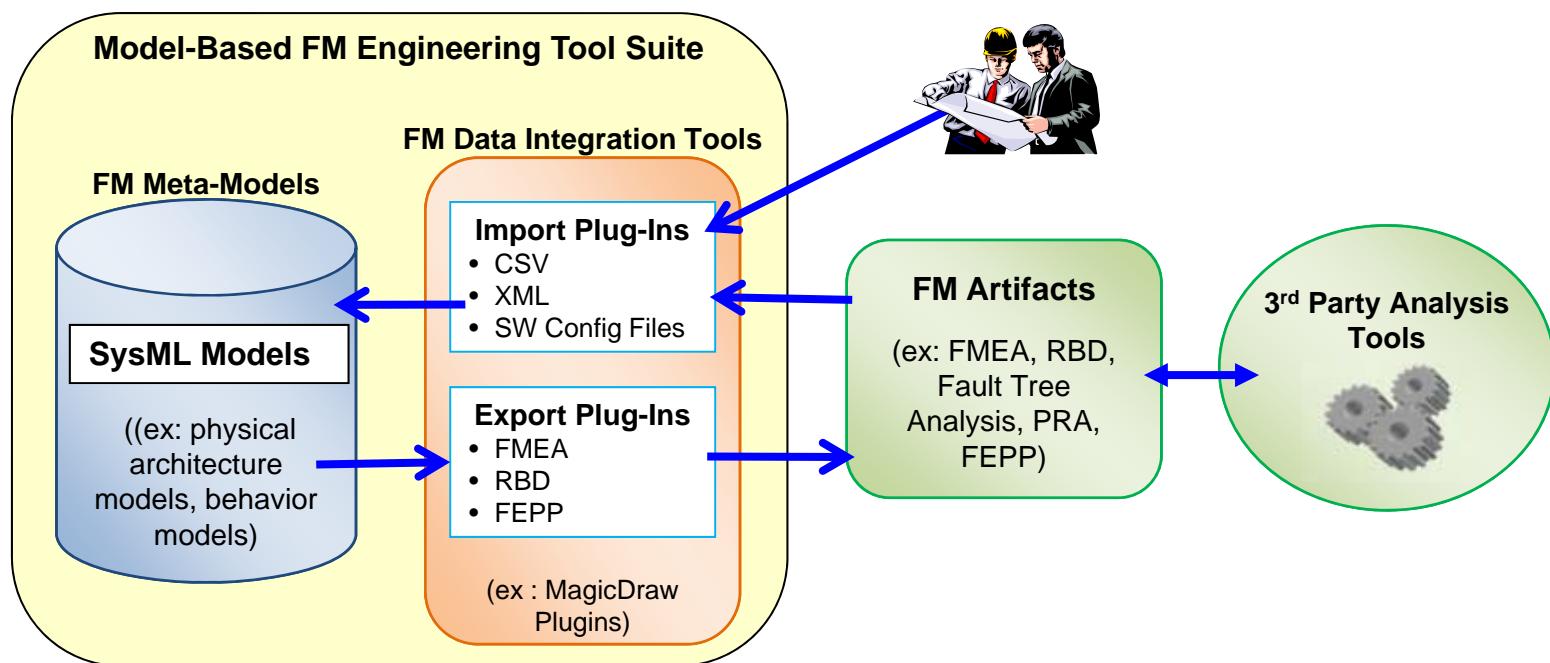
Model once and Use many times



MBFME Tool Suite Concept

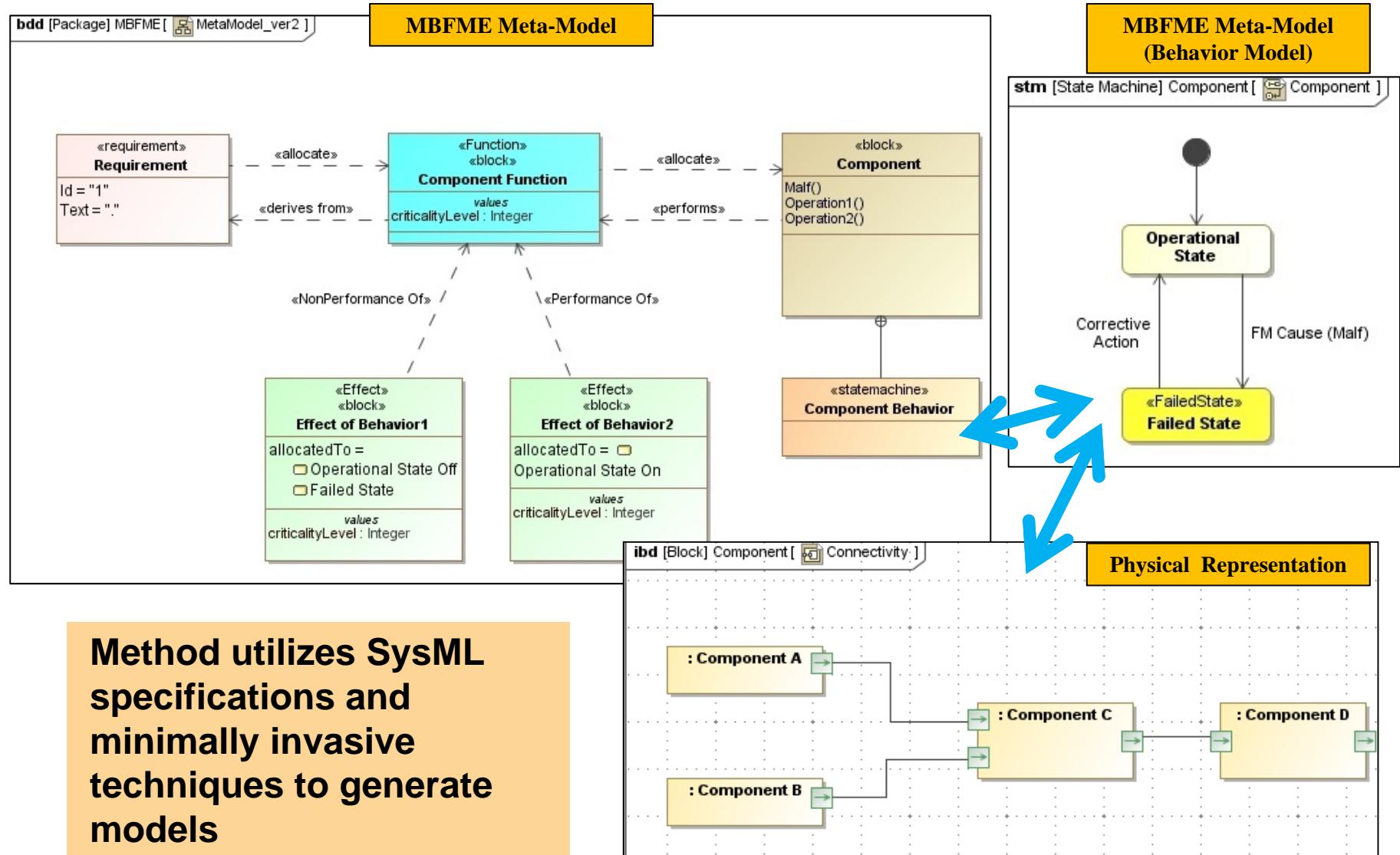


Model based Fault Management Engineering (MBFME)





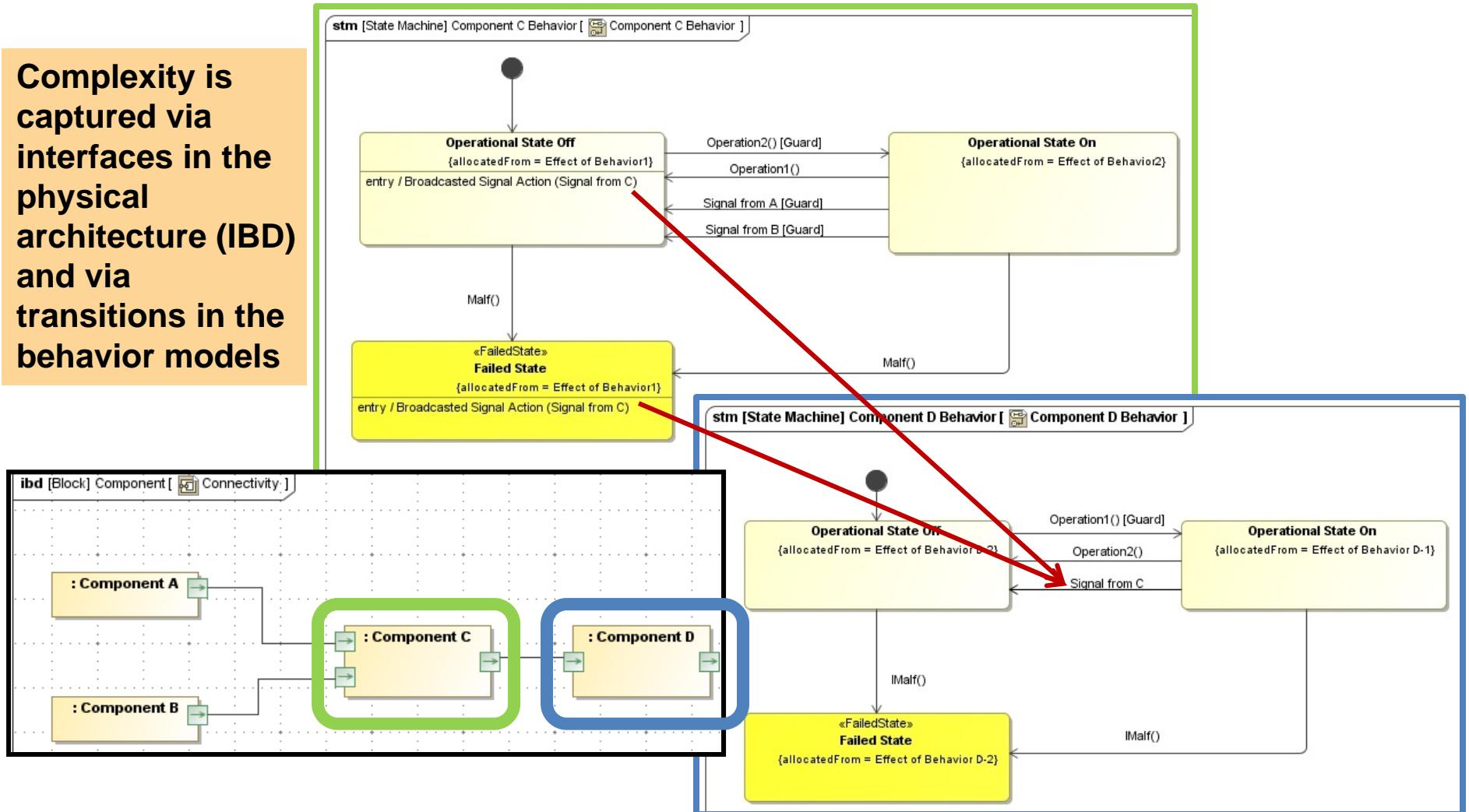
MBFME Meta-Model



MBFME Meta-Model (System Behavior)



Complexity is captured via interfaces in the physical architecture (IBD) and via transitions in the behavior models

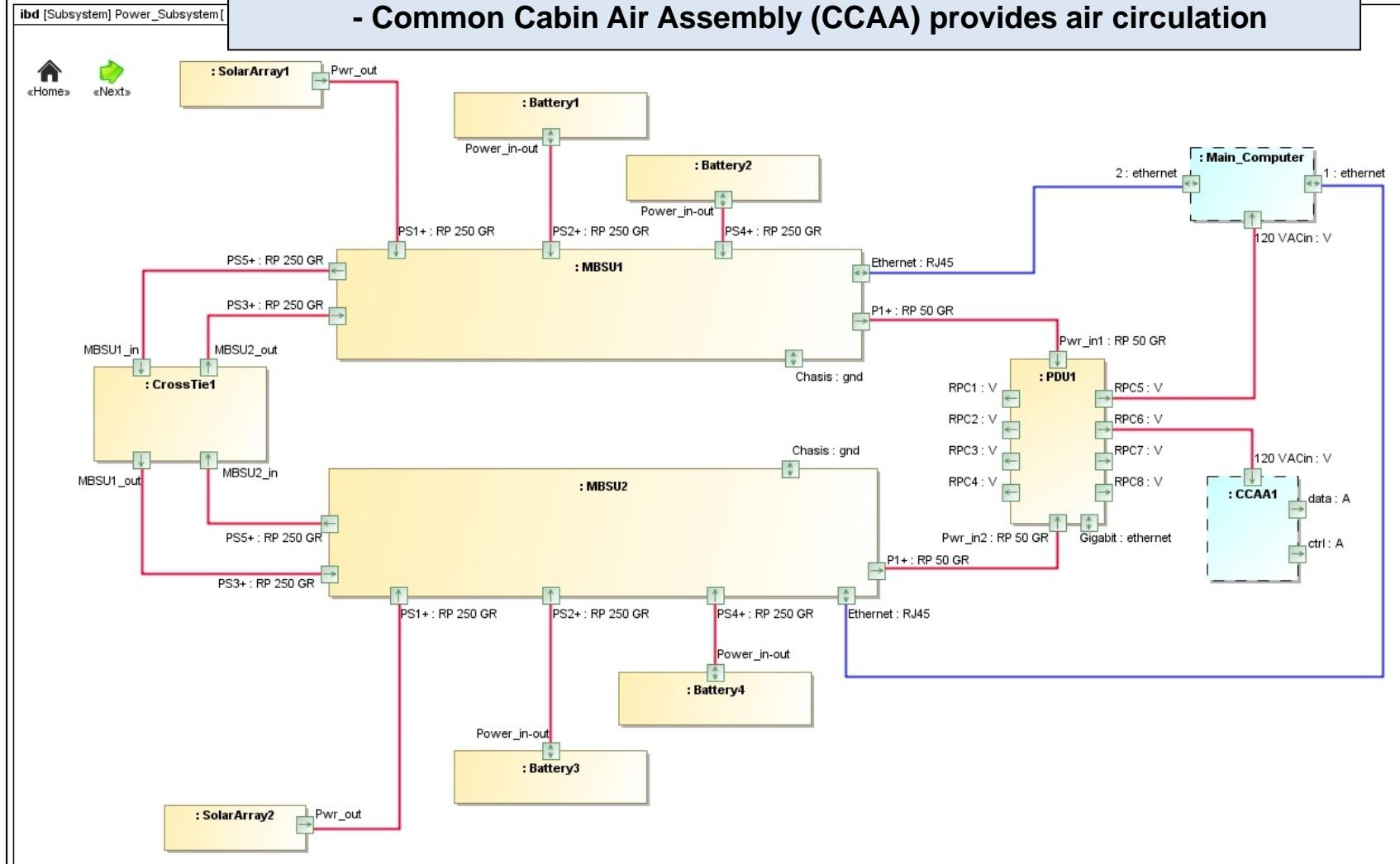


Power Subsystem Internal Block Diagram (IBD)



Applied MBFME Methodology to the Fan in the Can SysML model

- References a NASA spacecraft power architecture
- Contains 3 Subsystems (Power System, ECLSS, C&DH System)
 - Common Cabin Air Assembly (CCAA) provides air circulation

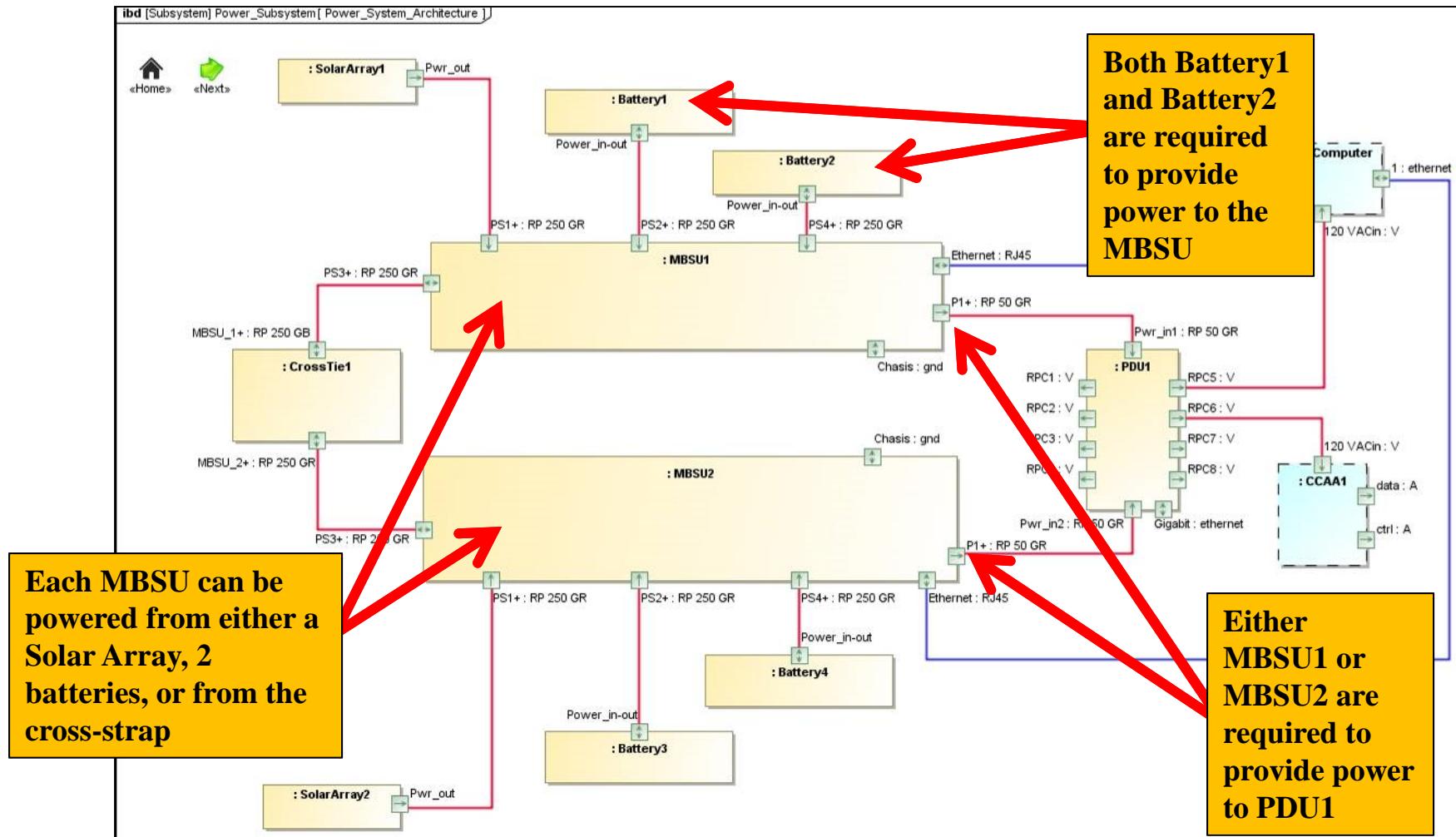




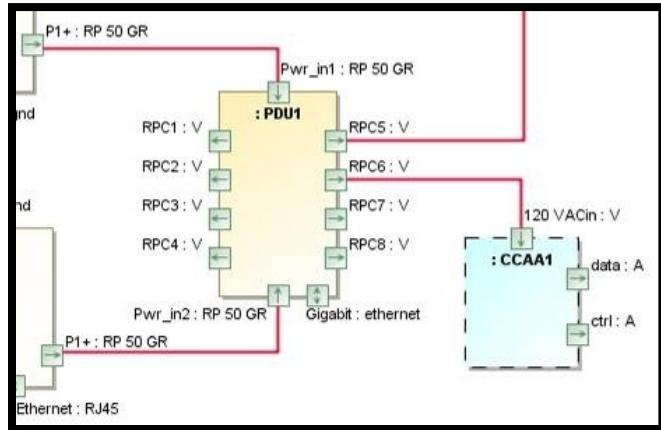
Power Subsystem Internal Block Diagram (IBD)

Fan in the Can SysML model

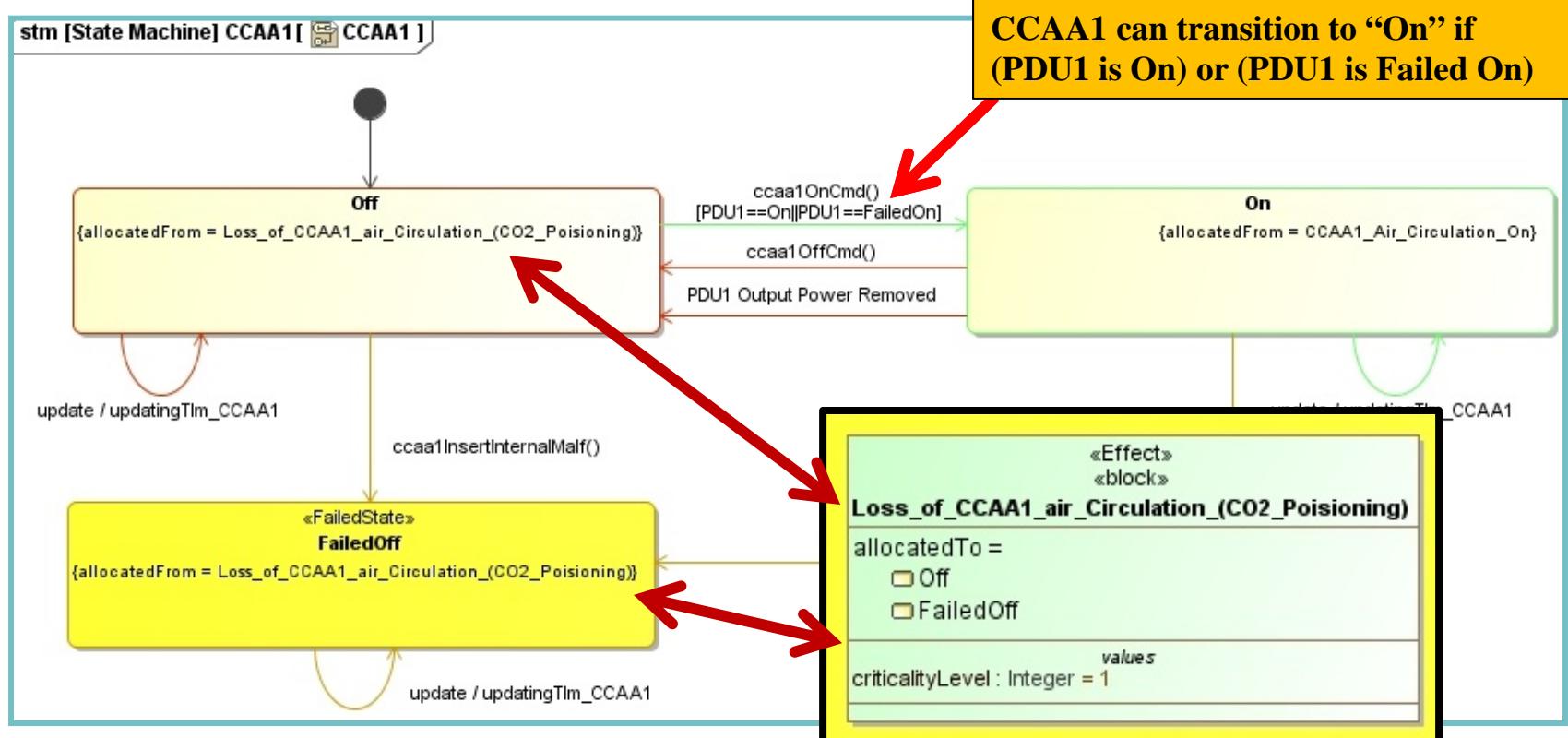
- Demonstrates redundancy in the power system
- Demonstrates power cross-strapping



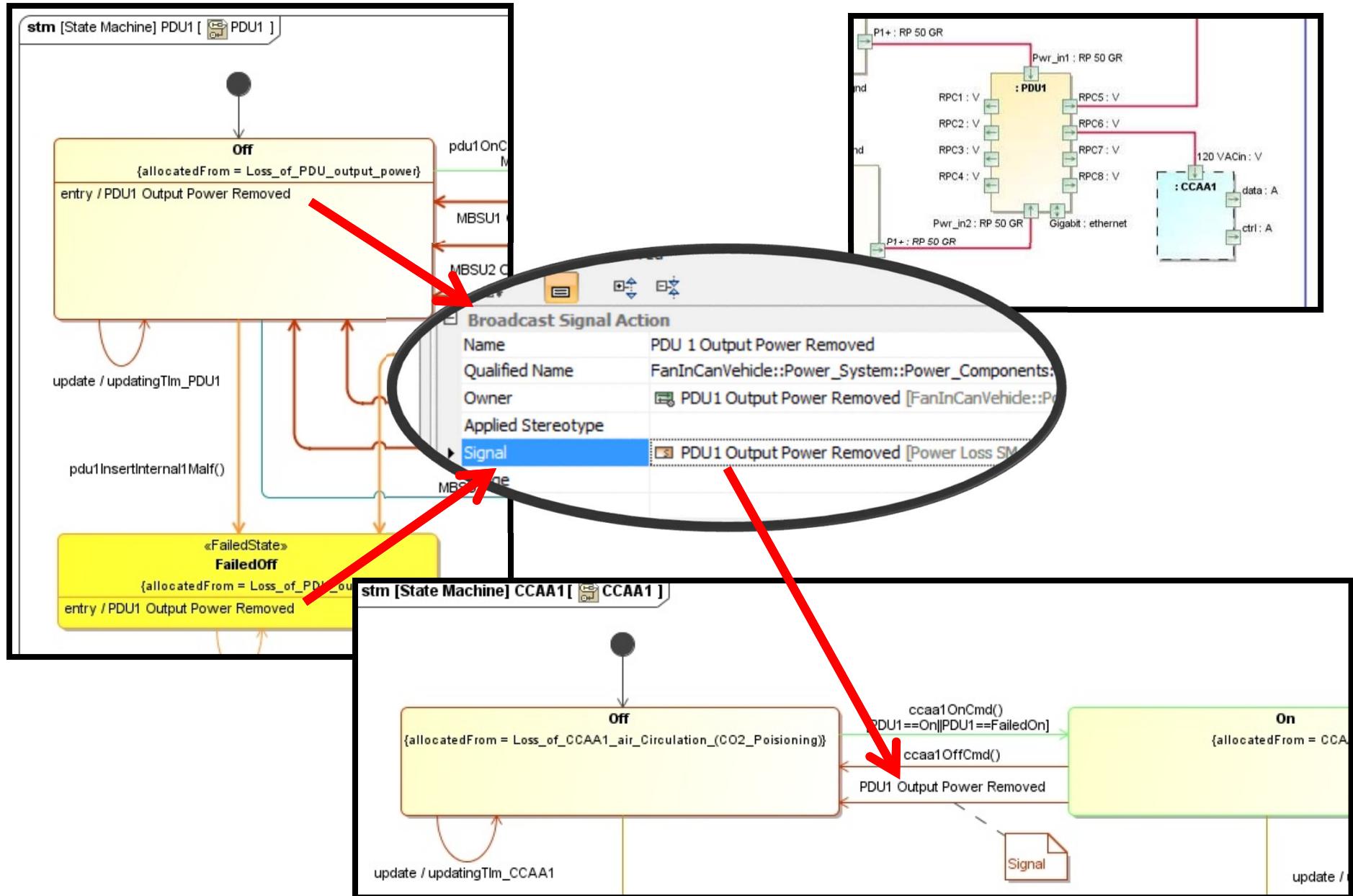
State Machine Diagram for CCAA1



- A Common Cabin Air Assembly (CCAA) function is to provide air circulation
- Loss of the CCAA1's function can result in loss of crew; Assigned a criticality level of 1.



Interactions Between PDU1 and CCAA1



FMECA (Failure Mode and Effects Criticality Analysis) Data Exchange



Magic Draw Plug-Ins

FMECA Output

SysML Models

The diagram illustrates the integration of FMECA analysis with SysML models. A red arrow points from the 'Run the Fmeaca Plugin' button in the Magic Draw interface to the FMECA output table below. Another red arrow points from the FMECA output table to the SysML models, indicating the exchange of data between the two domains.

FMECA Output

Failure Modes and Effects Criticality Analysis (FMECA)											
Project Name: Fan in the Can SysML Model											
System	Subsystem	LRU/ Assembly Type	LRU/ Assembly Name	Item Function	Potential Failure Mode	Effect			CRIT LEVEL	SEV	Potential Causes
						Immediate Failure Effect	End Effect	Number of Independent			
FaninCan	ECLSS	CCAA	CCAA1	CCAA1 Circulates Air	Failed Off	Loss of CCAA1 air Circulation	Loss of CCAA1 air Circulation	1		1	Internal Malf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed Off	Loss_of_Mbsu1_output_power	Loss of CCAA1 air Circulation	2	MBSU2 Failed Off	1	insertInternalMalf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed On	MBSU1_Ouput_Power_On					insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed On	Loss_of_ability_to_manage_MBSU1_loads					insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed Off	Loss_of_Mbsu2_output_power	Loss of CCAA1 air Circulation	2	MBSU1 Failed Off	1	insertInternalMalf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed On	MBSU2_Ouput_Power_On					insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed On	Loss_of_ability_to_manage_MBSU2_loads					insertInternal2Malf
FaninCan	Power Subsystem	PDU	PDU1	PDU_Distribute_Power	Failed Off	Loss_of_PDU_output_power	Loss of CCAA1 air Circulation	1		1	insertInternalMalf
FaninCan	Power Subsystem	PDU	PDU1	PDU_Distribute_Power	Failed On	PDU_Output_Power_On					insertInternal2Malf

SysML Models

The SysML models section shows three diagrams:

- bdd [Package] MBFME [MetaModel_ver2]:** A package diagram showing the allocation of requirements to functions and behaviors, and the allocation of behaviors to components.
- stm [State Machine] Component [Component]:** A state machine diagram for a component, showing states like Operational State, Failed State, and Faded State, along with transitions for Corrective Action and FM Cause (Malf).
- ibd [Block] Component [Connectivity]:** A block diagram showing the connectivity between components A, B, C, and D.

 Blue arrows indicate the flow of data or relationships between these models and the FMECA output table.



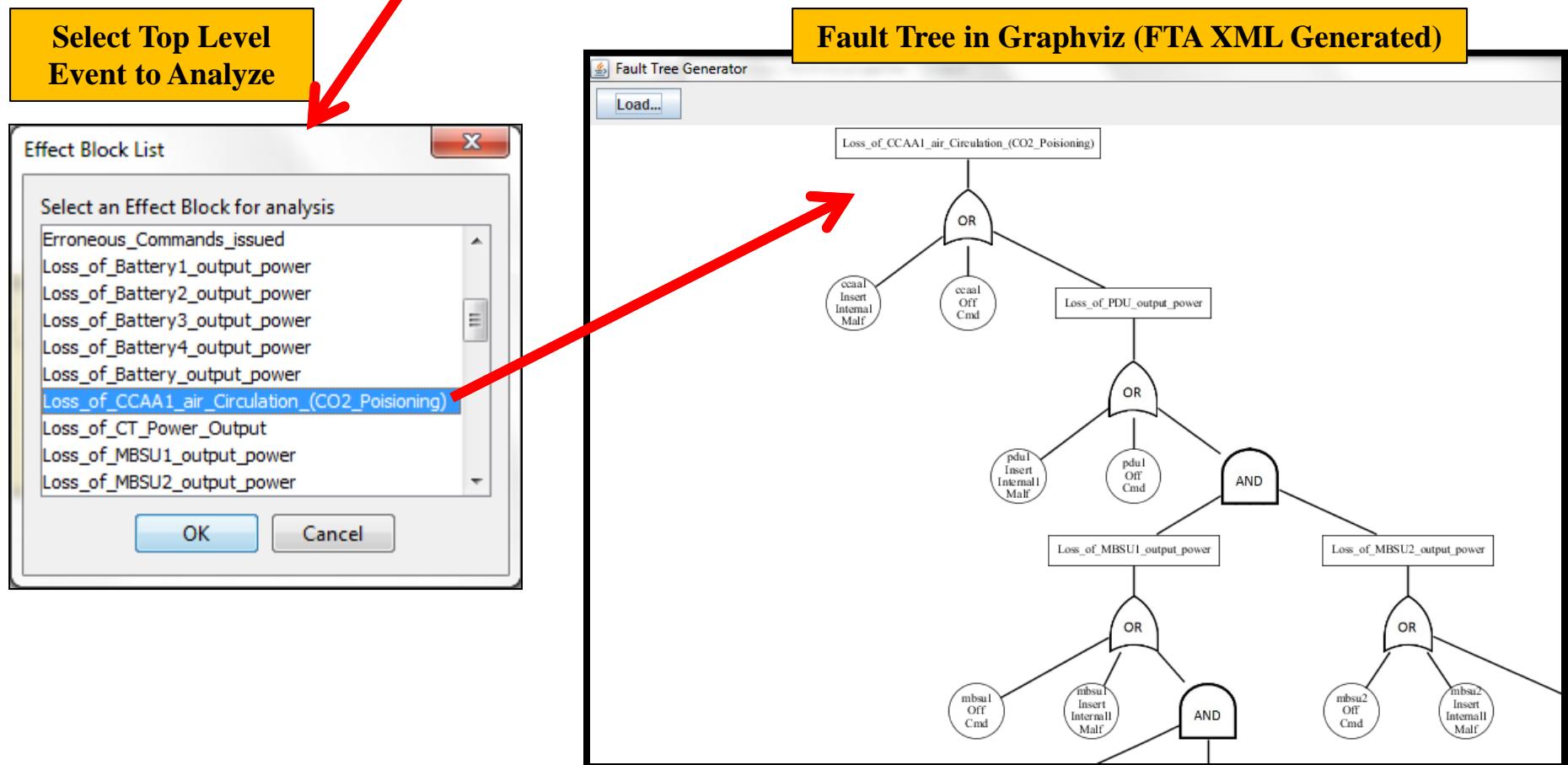
FMECA Analysis Results

- 10 Failure Modes Can Result in a Critical 1 Level Failure
- Due to redundancy (initial analysis without crosstie):
 - 6 potential failure modes are 2-fault tolerant
 - 2 potential failure modes are 1-fault tolerant
- The failure of the CCAA1 and PDU1 are critical failures requiring reliability measures

1	Failure Modes and Effects Criticality Analysis (FMECA)				
2	Project Name: Fan in the Can SysML Model				
3					
4					

8	System	Subsystem	LRU/ Assembly Type	Item Function	Potential Failure Mode	Effect					CRIT LEVEL	SEV	Potential Causes
						Immediate Failure Effect	End Effect	Number of Independent Failures	Other Independent Failures				
9	FanInCan	Power_Subsy stem	AMPS_PDU	PDU1	PDU_Distribute_Power	FailedOff	Loss_of_PDU_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	1		1		pdu1InsertInternal1Malf
10	FanInCan	ECLSS	CCAA	CCAA1	CCAA1_Circulate_Air	FailedOff	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	1		1		ccaa1InsertInternalMalf
11	FanInCan	Power_Subsy stem	AMPS_MBSU	MBSU1	MBSU_Distribute_Power	FailedOff	Loss_of_MBSU1_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	2	MBSU2 FailedOff	1		mbsu1InsertInternal1Malf
12	FanInCan	Power_Subsy stem	AMPS_MBSU	MBSU2	MBSU_Distribute_Power	FailedOff	Loss_of_MBSU2_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	2	MBSU1 FailedOff	1		mbsu2InsertInternal1Malf
13	FanInCan	Power_Subsy stem	AMPS_Solar_Array	SolarArray1	SA1_Generate_Power_SA_8.1_Generate_Power	FailedOff	Loss_of_SA1_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	3	(Battery1 FailedOff OR Battery2 FailedOff),MBSU2 FailedOff	1		solarArray1InsertInternalMalf
14	FanInCan	Power_Subsy stem	AMPS_Solar_Array	SolarArray2	SA2_Generate_Power_SA_8.1_Generate_Power	FailedOff	Loss_of_SA2_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	3	(Battery3 FailedOff OR Battery4 FailedOff),MBSU1 FailedOff	1		solarArray2InsertInternalMalf
15	FanInCan	Power_Subsy stem	AMPS_Modular_Lithium_Battery	Battery1	Battery_Generate_Power	FailedOff	Loss_of_Battery1_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	3	SolarArray1 FailedOff,MBSU2 FailedOff	1		battery1InsertInternalMalf
16	FanInCan	Power_Subsy stem	AMPS_Modular_Lithium_Battery	Battery2	Battery_Generate_Power	FailedOff	Loss_of_Battery2_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	3	SolarArray1 FailedOff,MBSU2 FailedOff	1		battery2InsertInternalMalf
17	FanInCan	Power_Subsy stem	AMPS_Modular_Lithium_Battery	Battery3	Battery_Generate_Power	FailedOff	Loss_of_Battery3_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	3	SolarArray2 FailedOff,MBSU1 FailedOff	1		battery3InsertInternalMalf
18	FanInCan	Power_Subsy stem	AMPS_Modular_Lithium_Battery	Battery4	Battery_Generate_Power	FailedOff	Loss_of_Battery4_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	3	SolarArray2 FailedOff,MBSU1 FailedOff	1		battery4InsertInternalMalf
19	FanInCan	Power_Subsy stem	AMPS_MBSU	MBSU1	MBSU_Distribute_Power	FailedOn	Loss_of_ability_to_manage_MBSU_loads						mbsu1InsertInternal2Malf
20	FanInCan	Power_Subsy stem	AMPS_MBSU	MBSU1	MBSU_Distribute_Power	FailedOn	MBSU1_Output_Power_On						mbsu1InsertInternal2Malf
21	FanInCan	Power_Subsy stem	AMPS_MBSU	MBSU2	MBSU_Distribute_Power	FailedOn	Loss_of_ability_to_manage_MBSU2_loads						mbsu2InsertInternal2Malf
22	FanInCan	Power_Subsy stem	AMPS_MBSU	MBSU2	MBSU_Distribute_Power	FailedOn	MBSU2_Output_Power_On						mbsu2InsertInternal2Malf
23	FanInCan	Power_Subsy stem	AMPS_PDU	PDU1	PDU_Distribute	FailedOn	PDU_Output_Power_On						pdu1InsertInternal

FTA (Fault Tree Analysis) Data Exchange



Future Directions / Conclusions

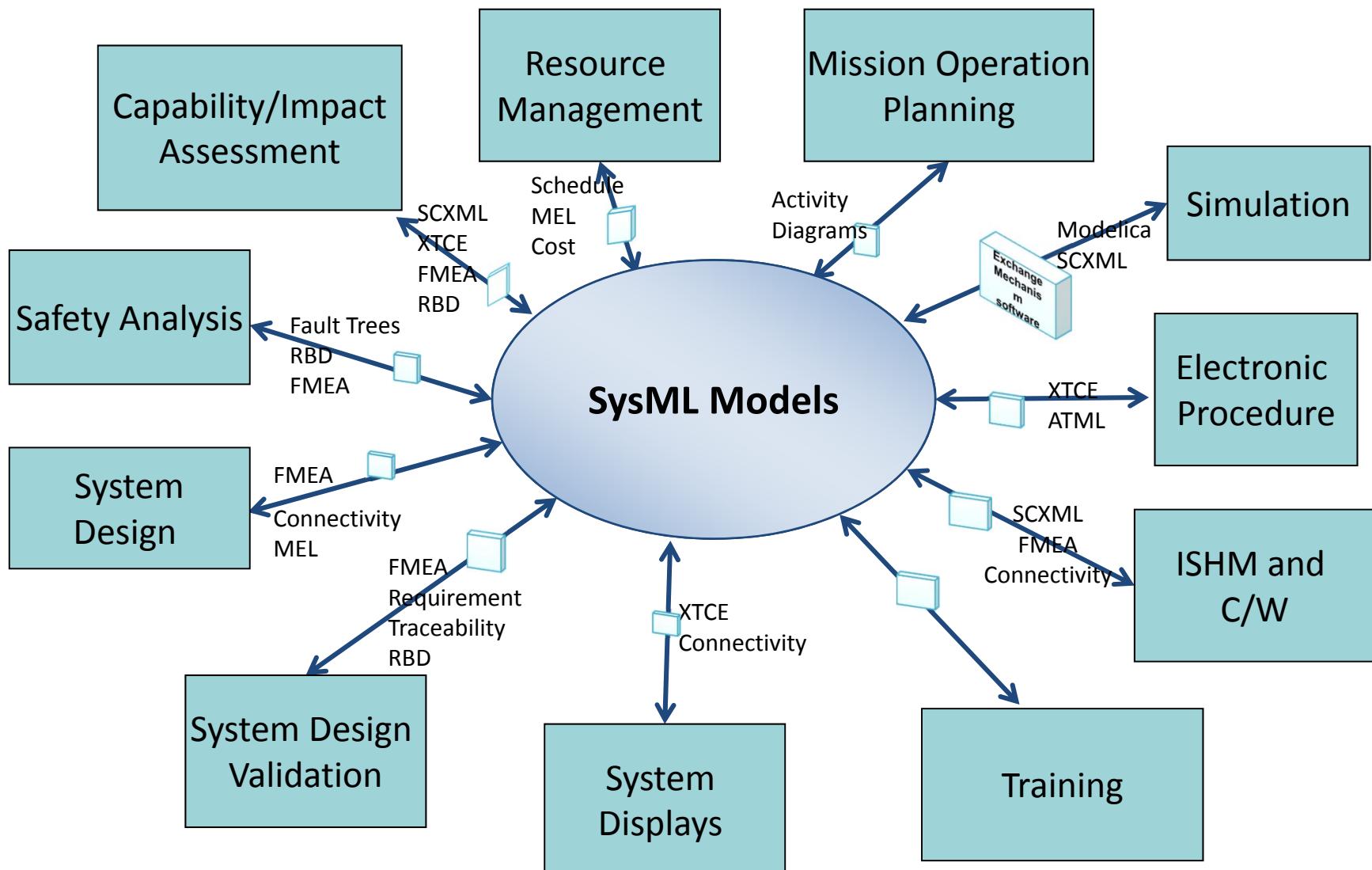


- ◆ Expand the FM meta-models (model attributes) to support additional FM products
- ◆ Continue collaboration with additional FM analysis experts (e.g., QSI TEAMS)
- ◆ Demonstrate the tools on NASA systems of varying complexity (e.g., CDS 2.0)
- ◆ Support automated generation of simulations with failure injection



Uses of System Models

Model once and Use many times



Backup Slides





Generate MEL from SysML

SysML Models

Magic Draw Plug-Ins

Generate MEL

MEL

The diagram illustrates the process of generating an MEL (Maintenance Item List) from a SysML model. A red arrow points from the "Generate MEL" button in the Magic Draw interface to the MEL table below. Another red arrow points from the "MEL" button to the table.

SysML Model Structure:

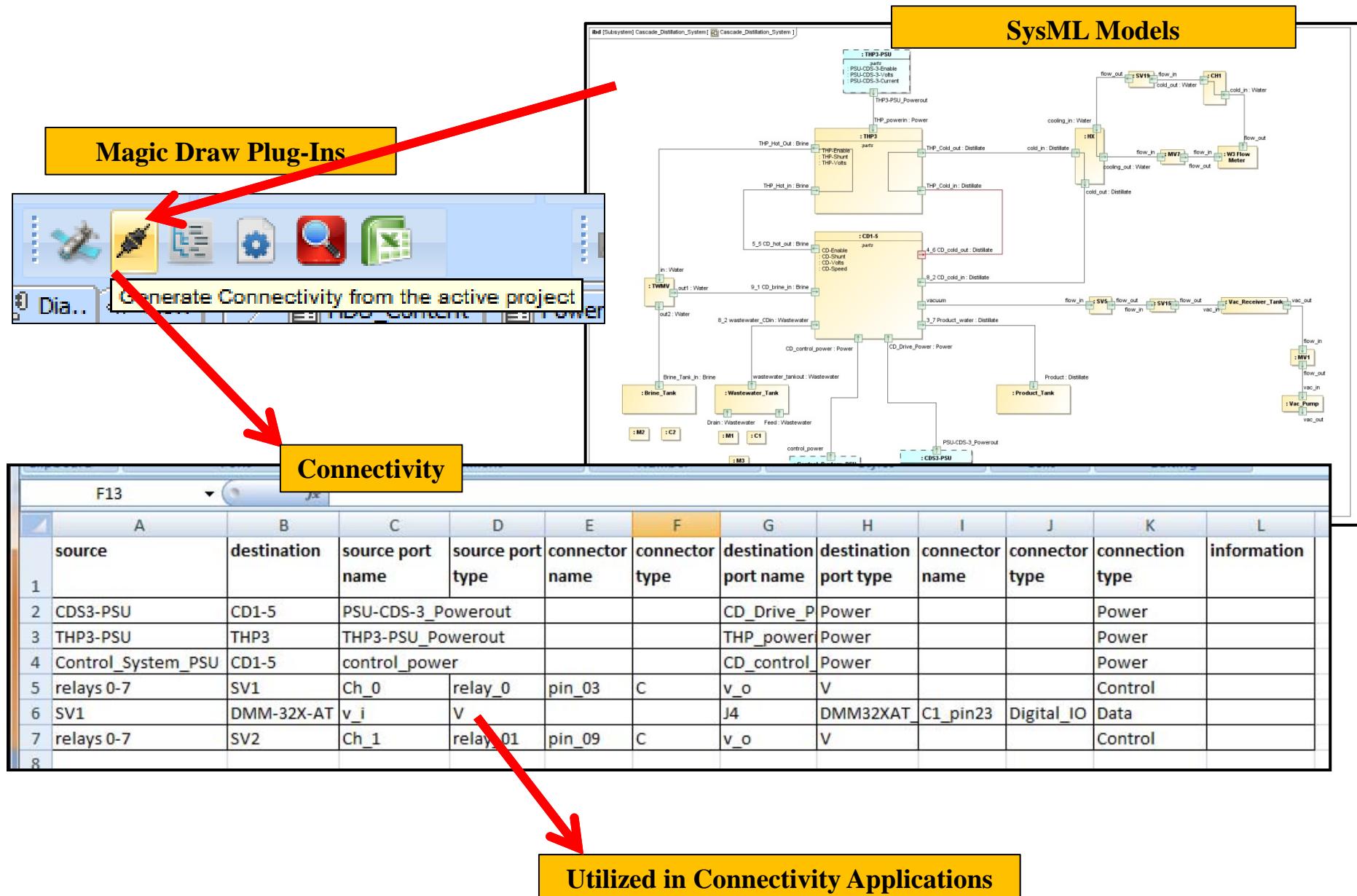
- Root Subsystem:** Cascade_Distillation_System
- Parts:**
 - Control_System_PSU**: An Assembly block containing parts CD1-5 and THP3.
 - CD1-5**: A Component block with attributes CD-Enable, CD-Shunt, CD-Volts, and CD-Speed.
 - THP3**: A Component block with attributes THP-Enable, THP-Shunt, THP-Volts.
 - Brine_Tank**: A Component block.
 - Product_Tank**: A Component block.
 - Wastewater_Tank**: A Component block.
 - Heat_Pump**: A Component block with attributes dP_Cold_Side, dP_Hot_Side, and gpm_Cold_Side.
 - Tank**: A Component block with attribute Mass.
- Subsystems:**
 - CDS_C&DH**: A subsystem with part CDS_UMC.
 - Facility_C&DH**: A subsystem with part FAC_UMC.
 - UPS-CDS-1**: A component.
 - UPS-CDS-2**: A component.
 - CDS3-PSU**: A component with part PSU-CDS-3-Enable.

MEL Table:

Items	Item Type		
CDS-PMM-1	Pearl MM relay	CDS_C&DH/C&DH_System	LRU
CDS-PMM-2	Pearl MM relay	C&DH_System/Facility_C&DH	LRU
FAC-PMM-1	Pearl MM relay	CDS_C&DH/C&DH_System	LRU
CDS-SM518-1	Sensoray 518	CDS_C&DH/C&DH_System	LRU
CDS-SM518-2	Sensoray 518	CDS_C&DH/C&DH_System	LRU
CDS-SM518-3	Sensoray 518	CDS_C&DH/C&DH_System	LRU
FAC-SM518-1	Sensoray 518	Facility_C&DH/C&DH_System	LRU
FAC-D32XAT-1	DMM-32X-AT	C&DH_System/Facility_C&DH	LRU
CDS-D32XAT-1	DMM-32X-AT	C&DH_System/CDS_C&DH	LRU
CDS-JMV512-1	Power Supply Board	CDS_C&DH/C&DH_System	LRU
FAC-JMV512-1	Power Supply Board	Facility_C&DH/C&DH_System	LRU
CDS-MIP405-1	CPU	CDS_C&DH/C&DH_System	LRU
FAC-MIP405-1	CPU	Facility_C&DH/C&DH_System	LRU
CDS-T16-1	AC bus termination board	CDS_C&DH/C&DH_System	LRU
FAC-T16-1	AC bus termination board	Facility_C&DH/C&DH_System	LRU
CD1-5	Cascade_Distiller	Cascade_Distillation_System/Water_Recover...	Assembly
THP3	Heat_Pump	Cascade_Distillation_System/Water_Recover...	Assembly
CDS_UMC	Universal_Micro_Controller	CDS_C&DH/C&DH_System	Assembly
FAC_UMC	Universal_Micro_Controller	Facility_C&DH/C&DH_System	Assembly
C1	Conductivity_Sensor	Cascade_Distillation_System/Water_Recover...	Component
C2	Conductivity_Sensor	Cascade_Distillation_System/Water_Recover...	Component

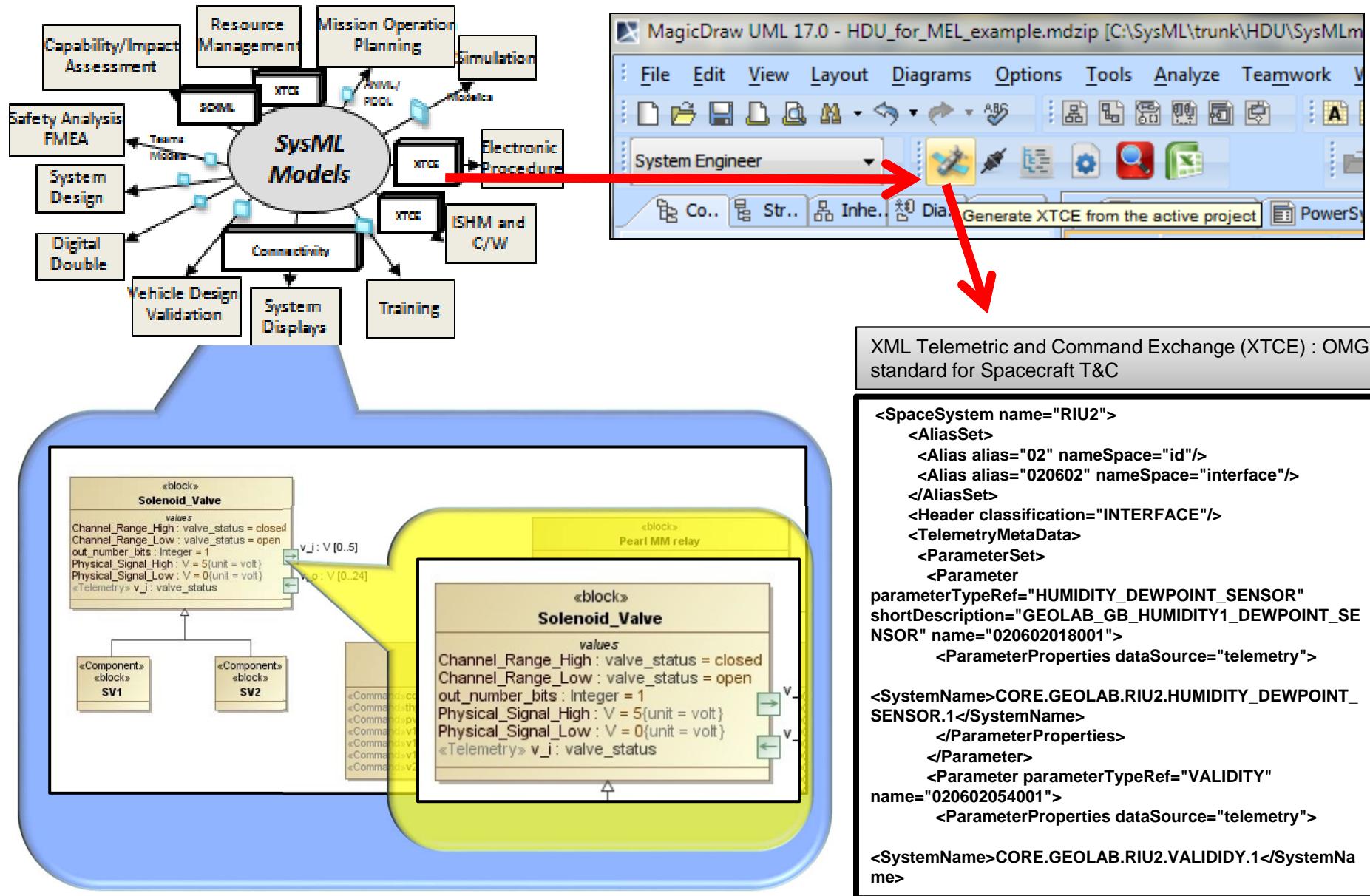


Connectivity Data Exchange



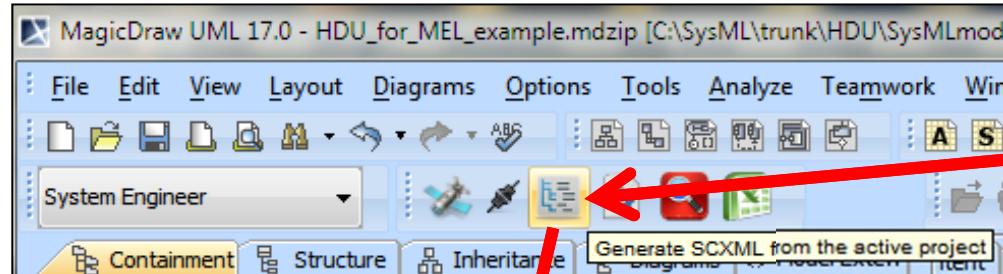


XTCE Exchange

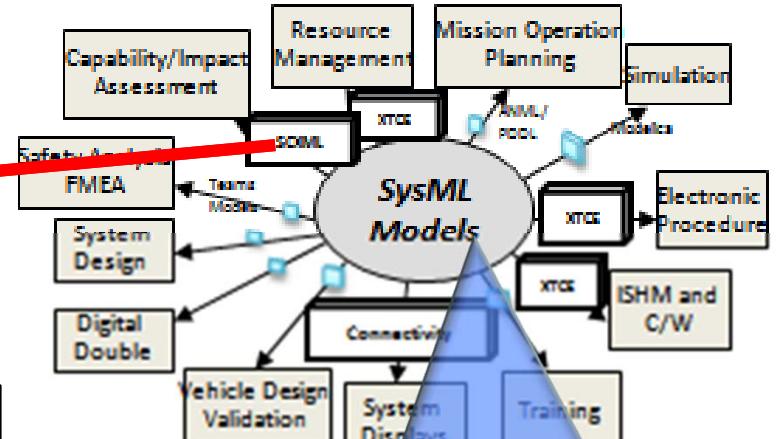




State Machine (SCXML)/FSM Exchange



SCXML: "State Chart extensible Markup Language". Provides a generic state-machine based execution environment based on Harel State Tables.

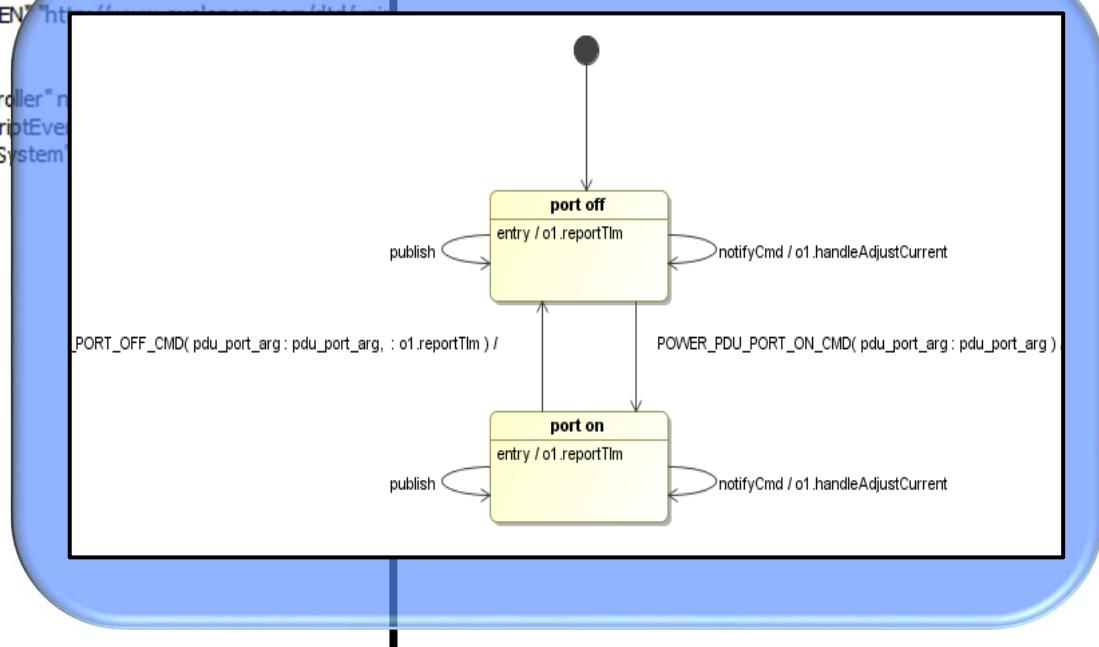


The code editor displays the XML configuration for the PowerSystem state machine:

```

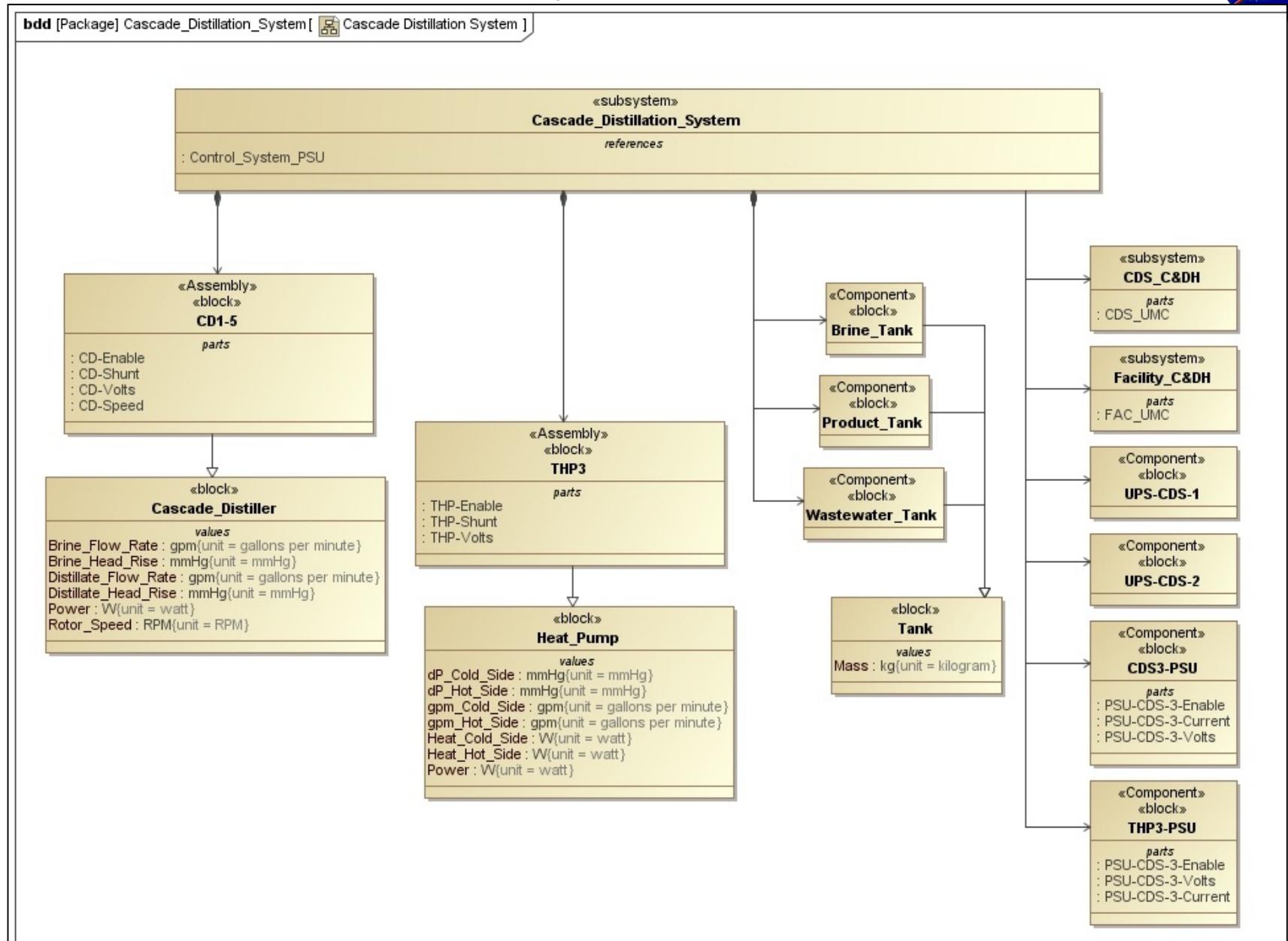
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE model PUBLIC "-//eDevelopers Corp.//DTD State machine model V1.0//EN" "http://www.evelopers.com/DTD/SMV1.0.dtd">
<model name="Data">
<controlledObject class="com.tietronix.controllers.PowerSystemInterfaceController" name="PowerSystem">
<eventProvider class="com.evelopers.unimod.adapter.standalone.provider.ScriptEventProvider" clientRole="p1" supplierRole="PowerSystem" targetRef="PowerSystem"/>
</eventProvider>
<rootStateMachine>
<stateMachineRef name="PowerSystem"/>
</rootStateMachine>
<stateMachine name="PowerSystem">
<state name="TOP" type="NORMAL">
<state name="s1" type="INITIAL"/>
<state name="Running" type="NORMAL">
<stateMachineRef name="pdu"/>
<stateMachineRef name="rpc"/>
</state>
</state>
<transition name="" sourceRef="s1" targetRef="Running"/>
</stateMachine>
<stateMachine name="bank1">
<association clientRole="bank1" supplierRole="o1" targetRef="o1"/>
<state name="TOP" type="NORMAL">

```





CDS System Model





Concept of Operations

